Android Memory Forensics

Degree programme : MAS Digital Forensics & Cyber Investigation

In recent years, mobile devices have become increasingly important in daily life. Today, it is almost impossible to imagine life without them. With the growing importance, the interest of criminals and malware programmers in these devices is also rising. Subsequently, mobile devices are becoming targets for criminals and therefore objects of interest for investigators. This master thesis presents which possibilities exist to examine the volatile memory of Android devices.

For security managers in large companies or organizations, bring your own device (BYOD) policies is a topic of genuine concern.

This thesis shows that the evaluation of the volatile memory of Android phones is still problematic, respectively increasingly getting more problematic. With each phone, new security features are added, which also make it more burdensome for investigators and forensic practitioners to access this type of data.

However, it could also be shown that the effort can be worthwhile, as information can be found in the volatile memory that is very challenging to obtain otherwise. Using the app Threema, it was shown that both the individual messages and the passphrase can be found in the memory. In other experiments indicators of compromise such as command & control server of malware could also be found in memory.

Commercial products offer few solutions. At best, they carve known file types such as images or database metadata from a memory image. Only few makers seem to extend their products to evaluate volatile memory. One of them recently added a new feature to evaluate health data from the volatile memory of Samsung devices. Since Samsung is by far the best-selling brand of Android cell phones in Switzerland, this could be of interest to investigators. If a device has not been prepared in advance, the investigators have very few options. However, some Samsung devices in particular offer the possibility to read out parts of the memory without changing the device significantly or even rooting it.

The situation for companies and organizations is not very rosy either. Mobile Device Management (MDM) products do not offer a solution for the evaluation of volatile memory. It would be conceivable to adapt the phones that are handed over to employees in such a way that the corresponding tools can be executed with root rights if required. For this, the phone would at least have to be unlocked. This in turn would open additional attack vectors, which increase the risk of attacks. The additional risks do not justify the gain in functionality.

Regarding malware analyze memory forensics might support a researcher in the process of analyze a specific malware. Yet the lack of analyzing the memory dump with tools like Volatility does limit the information expected to be gained.

Michael Herren
michael@beMe.ch